REMARKS

Reconsideration of the application is respectfully requested for the following reasons:

1. Objection to Specification

This objection has been addressed by amending paragraph [022] of the original specification to clarify that the "means" recited in original claims 5 and 6 corresponds to the software routine illustrated in Fig. 6, which "creates" a call-info table to track certain INVITE messages (based on whether the INVITE messages have credentials and whether call-info is present in the call-info table). The added materials added to paragraph [022] of the specification correspond to the original claim language, including use of the term "means," and therefore do not involve "new matter."

It is respectfully noted that claims 7 and 8 have been added to recite the creation of the cal-info table, as described in original paragraph [022]. New claims 7 and 8 therefore also do not involve "new matter."

2. Claim Objections

This objection has been addressed by amending the claims in the manner suggested by the Examiner on pages 2-3 of the Official Action, and by making additional changes to improve readability. These amendments correct informalities and therefore do not involve "new matter."

3. Rejection of Claim 4 Under 35 USC §112, 1st Paragraph

This rejection has been rendered moot by the cancellation of claim 4.

4. Rejection of Claims 1, 2, 5, and 6 Under 35 USC §112, 2nd Paragraph

This rejection has been addressed as follow:

- Claim 1 has been amended to specify that the indication of the presence of a current DoS attack is based on detection of an imbalance between INVITE and 180 messages

resulting from a DoS attack, the INVITE and 180 messages being SIP protocol messages. Claim 1 is now complete unambiguous since INVITE and 180 messages are specific message types defined by the SIP protocol, and since the imbalance is now limited to imbalances caused by DoS attacks rather than trivial imbalances caused by phones that are off-the-hook and the like.

- Claim 6 has also been amended to clarify that the imbalance is one caused by a DoS attack, and that the INVITE and 180 messages are specific types of messages defined by the SIP protocol.
- Claim 2 has been amended to positively recite that the variables INV_o and INV_c respectively indicate the number of INVITE messages without credentials and the number of INVITE messages with credentials, and also to positively recite that the variable N_{180} represents the number of ringing messages defined in claim 1.
- Claim 2 has also been amended by deleting the indefinite term "small" and by defining the "credentials" as authenticating information, as would be well-known to those skilled in the art.
- Claim 5 has been amended to complete the "if" clause by reciting that the proxy server includes means for determining if the number of INVITE messages including credentials (INV_c) sent to said proxy server *exceeds a predetermined level*.
- Claim 5 has been further amended to recite that it is the determination that the number of INVITE messages with credentials exceeds the predetermined level that indicates whether a DoS attack has occurred, thereby eliminating the recitation of "providing an indication" and the need for a separate "means."
- Claim 6 has been amended to recite that it is the imbalance that indicates the existence of a DoS attack, thereby providing a basis for the recited "indication."
- Finally, the specification has been amended as noted above to provide antecedence for the claimed "means." In particular, the claimed "means" are now supported by the description in paragraph [022] of the software routine illustrated in Fig. 6.

4. Double Patenting Rejection

This rejection is respectfully traversed on the grounds that none of the claims of copending Application No. 10/849,830 (the copending application) recite detection of SIP INVITE and/or SIP 180 Ringing messages as an indication of DoS attacks, as presently claimed, and on the grounds that the present invention is not an obvious variation of what is claimed in the copending application. In fact, the '830 application deals with an entirely different problem than the present application, and arrives at an entirely different solution.

According to the present invention, "denial of service" or DoS attacks on a SIP proxy server are detected by, in effect, comparing the number of call requests (INVITE messages) with the number times a phone rings in response to the call requests (180 Ringing messages). This works because DoS attacks seek to overwhelm the server with more call requests than can be responded to by ringing, and which might not even be directed to an actual telephone connected to the system, so that an imbalance between requests (INVITE messages) and ringing (180 Ringing messages) actually does indicate an attack. The prior art described in Applicant's specification also compared INVITE messages, but the messages were compared with actual answered telephones rather than just ringing, resulting in a number of problems including the problem that an imbalance could result simply because users were not answering their phones, or because the requests were to non-existent phones.

The copending application, on the other hand, does not claim or even disclose detecting **DoS** attacks. Instead, the copending application concerns detecting spam messages, which are unwanted messages directed to a particular end user. **Spam** messages are annoying to the end user, but unlike a DoS attack are not intended to shut down or overwhelm a server. Furthermore, detection of spam messages, at least as disclosed and claimed in the copending application, does not involve the same solution as the presently claimed invention, namely comparison of INVITE and Ringing messages. Instead, the copending application discloses a solution involving comparing call set up (INVITE) requests with call **terminations** or "BYE" messages. The reason this works is that most spam calls are terminated relatively quickly, either by an annoyed

recipient upon determining that the call is a spam call, or by the spammer upon determining that the callee is not interested. Furthermore, the copending application discloses an alternative solution in which calls in one direction are compared with calls in another direction, which works because hardly anyone ever calls back a spammer. In either case, the solution has **nothing** to do with detecting DoS attacks on the server.

The claims of the copending application recite using "statistics" on incoming and outgoing calls and taking action to mitigate unsolicited calls. The claims do not recite either detection of DoS attacks or comparing INVITE messages with Ringing messages, and the disclosure of the copending application makes clear that the invention involves neither DoS attacks nor Ring messages. In fact, the claims of the copending application are directed to an entirely different and at best tangentially-related invention, and recite none of the features claimed in the present application. Accordingly, the double patenting rejection is believed to be improper and withdrawal of the rejection is respectfully requested.

5. Rejection of Claims 1-6 Under 35 USC §102(e) in view of U.S. Patent Publication No. 2003/043740 (March)

This rejection is respectfully traversed on the grounds that the March publication does not disclose or suggest detecting DoS attacks on a proxy server, as claimed, based on a comparison or accounting of **INVITE** message, which are call set-up requests, and **180 Ringing** messages which are generated when a telephony device connected to the network rings. To the contrary, the March patent merely discloses detection of DoS attacks based on the "**rate of incoming data units**," which is not even remotely suggestive of the claimed comparison.

Paragraph [0005] of the March publication, cited by the Examiner, discloses that DoS attacks are addressed by storing a "pattern or threshold for a communications session" and by "detecting that a ***rate of incoming data units*** exceeds the threshold or the ***incoming data units*** do not match the pattern." The "rate" of incoming data units exceeding a threshold is clearly not the same or analogous to the claimed **imbalance between set-ups (INVITE messages) and**

rings (Ringing messages), nor is the matching a "pattern" of incoming data units suggestive of the claimed imbalance. The Examiner will note that what is being monitored in March are **incoming data units**, and not set up of ringing messages. March monitors all data units. While a large number of incoming data units is certainly indicative of a denial of service attack, it might also simply indicate an unexpectedly high call volume, such as might occur during an emergency.

Paragraph [0029] of the March publication, also cited by the Examiner, is no more relevant than paragraph[0005]. This paragraph discloses that attacks are detected based on "a greater than expected amount of packets from the external network." Paragraph [0096], also cited by the Examiner, merely refers to "expected traffic patterns/thresholds on a per session basis. Neither of these paragraphs is as relevant as the prior art discussed in Applicant's own specification, which points out a prior attempt to detect DoS attacks by comparing INVITE messages with OK messages that indicate that a call has been answered. The claimed invention modifies this prior art by checking Ringing messages rather than OK messages. Since the March publication does not disclose any sort of call-set monitoring, much less comparison or accounting of SIP "INVITE" and "180 Ringing," the March publication could not possibly have suggested the claimed improvement over the prior art, and withdrawal of the rejection of claims 1-6 under 35 USC §103(a) is respectfully requested.

Having thus overcome each of the rejections made in the Official Action, withdrawal of the rejections and expedited passage of the application to issue is requested.

Respectfully submitted,

Date: March 12, 2008

By: Jim Zegeer, *Esq.*
Registration No. 18,957

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500